NOKIA

NSP
Network Services Platform

Network Functions Manager - Packet (NFM-P)

Release 20.3

Architecture Guide

3HE-16025-AAAA-TQZZA

Issue 1

March 2020

Legal notice

Contents

About this document

Purpose

The *NSP NFM-P Architecture Guide* is intended for technology officers, network planners, and system administrators to increase their knowledge of the NFM-P software structure and components. It describes the system structure, software components, and interfaces. In addition, NFM-P fault tolerance, security, and network management are described from an architectural perspective.

Scope

The scope of this document is limited to the NFM-P application. Many configuration, monitoring, and assurance functions that can be accomplished from the NFM-P Java GUI are also delivered in NSP web-based applications accessible from the NSP Launchpad. Readers of this NFM-P guide should familiarize themselves with the capabilities of the NSP applications, which often offer more efficient and sophisticated features for network and service management. Help for all installed NSP applications is available in the NSP Help Center.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Documentation feedback

1 NFM-P architecture

1.1 NFM-P architecture overview

1.1.1 Introduction

The NFM-P is a network management system that simplifies routine operations and allows the bulk provisioning of network objects. The system is designed using industry standards such as Java, XML/SOAP, REST, and WebDAV. The NFM-P uses open-standard interfaces that allow the system to interoperate with a variety of other network monitoring and management systems.

1.1.2 NFM-P functions

The NFM-P network management functions include the following:

- service and routing configuration using distributed policies and profiles
- equipment, service, and customer inventory reporting
- network performance, accounting, and flow-based statistics collection
- hierarchical alarm correlation between objects
- interworking with other network systems

1.1.3 Main architecture features

The main features of the NFM-P architecture include the following:

- the use of open standards to promote interaction with other systems
- distributed resources that spread the processing load across multiple components and efficiently execute network management tasks
- a multi-layer design model with functions in separate modules that interact with OEM products to accommodate increasing network growth and complexity
- web services that provide access to NFM-P applications by effectively exporting XML and REST interfaces over the Internet; the web services permit access to remote components such as web portals, and allow third-party vendors to create customized entry points for NFM-P functions
- component redundancy that provides a high degree of fault tolerance

1.2 Network management functions

1.2.1 Introduction

The NFM-P provides comprehensive network access for operators based on role-based scopes of command and spans of control over types of network objects.

An NFM-P system collects data from managed NEs and collates the data for accounting, performance monitoring, troubleshooting, inventory, and fault management. The system deploys operator commands to the network, and performs functions such as NE discovery and configuration backups.

An NFM-P system is primarily designed to manage proprietary devices. However, you can obtain drivers for managing some devices from other vendors. Drivers can be downloaded from the customer support site, and driver installation and usage documentation is available from the Documentation Center.

1.2.2 Service management

NFM-P service management allows network operators to provision customer services such as VLL, VLAN, VPLS, IES, and VPRN. Each service can be monitored to provide performance, usage, and fault information.

1.2.3 Accounting

The NFM-P collects accounting statistics from managed NEs. Depending on the deployment and required functions, the NFM-P stores, forwards, or performs post-processing on the collected statistics data. A variety of statistics reporting and presentation functions are available.

1.2.4 Equipment management

The NFM-P maintains an equipment data model and deploys configuration updates to the managed NEs. For example, when an NFM-P operator adds a card to an NE, the data model is updated to include the card, and the card provisioning and configuration commands are sent to the NE. New NEs can be discovered at operator request, or automatically. A newly discovered NE is added to the data model.

1.2.5 Performance management

The NFM-P can monitor services and network resources using performance statistics, OAM diagnostic tools, and data validation, and raises alarms when appropriate.

- The NFM-P can collect NE performance statistics and KPI information from specified NEs.
- The NFM-P has a comprehensive suite of OAM tools for monitoring service, NE, and transport availability and performance. You can also run tests before service activation to ensure that a service functions correctly after activation.
- The NFM-P regularly compares the configuration of each managed NE with the associated information in the NFM-P database, and updates the database information accordingly.

1.2.6 Fault management

The NFM-P performs fault management in response to NE events by analyzing the events to create status updates and raise alarms, as required. GUI clients use visual and auditory cues to alert an operator to a new alarm.

The NFM-P immediately forwards fault information as JMS events to OSS clients that subscribe to the appropriate JMS topic, and in response to XML API or REST API client requests for information.

1.3 System components

1.3.1 Introduction

An NFM-P system includes several components that are described below. Some components are supported only in specific deployment types. See the *NSP NFM-P Planning Guide* for comprehensive information about the supported deployment configurations.

1.3.2 Main server

A main server is the central Java-based network-management processing engine. A main server can be collocated on one station with a main database, or installed on a separate station. A main server includes third-party components such as an application server, JMS server, web server, protocol stack, and database adapter. Some functions, for example, statistics collection, can be distributed across optional auxiliary servers.

1.3.3 Auxiliary server

An auxiliary server, like a main server, is a Java-based processing engine, but is an optional, scalable component that extends the system ability to perform functions such as statistics, PCMD, or call-trace data collection. An auxiliary server is controlled by a main server, and collects data directly from NEs.

1.3.4 Main database

The main database is a customized relational database that provides persistent storage and serves as a central network data repository. The database can be collocated on one station with a main server, or installed on a separate station.

1.3.5 Auxiliary database

An auxiliary database is an optional, horizontally scalable database that expands the NFM-P storage capacity for demanding operations such as statistics collection, and performs data aggregation required by the NSP Analytics application.

The database is deployed on one station, or distributed among a cluster of three or more stations, depending on the scale requirement. In a multi-station auxiliary database, load balancing and data replication among the stations provide high performance and robust fault tolerance. An auxiliary database supports geographically redundant deployment, in which an auxiliary database cluster is deployed in each data center.

1.3.6 Single-user GUI client

A single-user GUI client is a Java-based graphical interface for network operators. Single-user GUI client deployment is supported on multiple platforms.

1.3.7 Client delegate server

A client delegate server supports simultaneous GUI sessions using one client software installation. A client delegate server can host local and remote user sessions, and supports the use of a third-party remote access tool such as a Citrix gateway. Client delegate server deployment is supported on multiple platforms.

A GUI session that is opened through a client delegate server is functionally identical to a single-user client GUI session. The client delegate server locally stores the files that are unique to each user, such as the client logs and GUI preference files.

1.3.8 OSS clients

An Online Support System, or OSS client, is an in-house or third-party application that automates GUI client tasks or retrieves data from the NFM-P. An OSS client is platform-independent, because only Java messages are exchanged with the NFM-P.

The NFM-P supports the following OSS clients:

- XML/SOAP clients—use the NFM-P XML API to perform network management; XML schema files provide the data object definitions and describe the object attributes and methods; see the *NSP NFM-P XML API Developer Guide* for information
- REST API clients—use the NFM-P REST API to perform network management; see the online REST API documentation for information

1.3.9 PCMP

The Protocol Converter and Mediation Platform, or PCMP, interacts with a 7750 SR that acts a virtual residential gateway, or vRGW. The PCMP translates REST API calls from a bridged residential gateway controller, or BRGC, into the configuration required to modify the operational behavior of bridged residential gateways, or BRGs, that are downstream from the 7750 SR.

vRGW

The vRGW is a 7750 SR BNG that performs the L3 functions of a routed residential gateway. The vRGW performs L3 functions such as address management, routing, IP connectivity, NAT, UPnP, firewalls, and parental controls. The residential gateway operates in bridge mode, which provides operator visibility of the connected devices on the home LAN. vRGW sometimes refers to the integrated 7750 SR and PCMP solution.

BRG

A BRG is a residential gateway for which L3 functions are handled by a vRGW. The BRG performs local switching of intra-home traffic that originates and terminates on devices within the home, and is a logical representation of the residential subscriber.

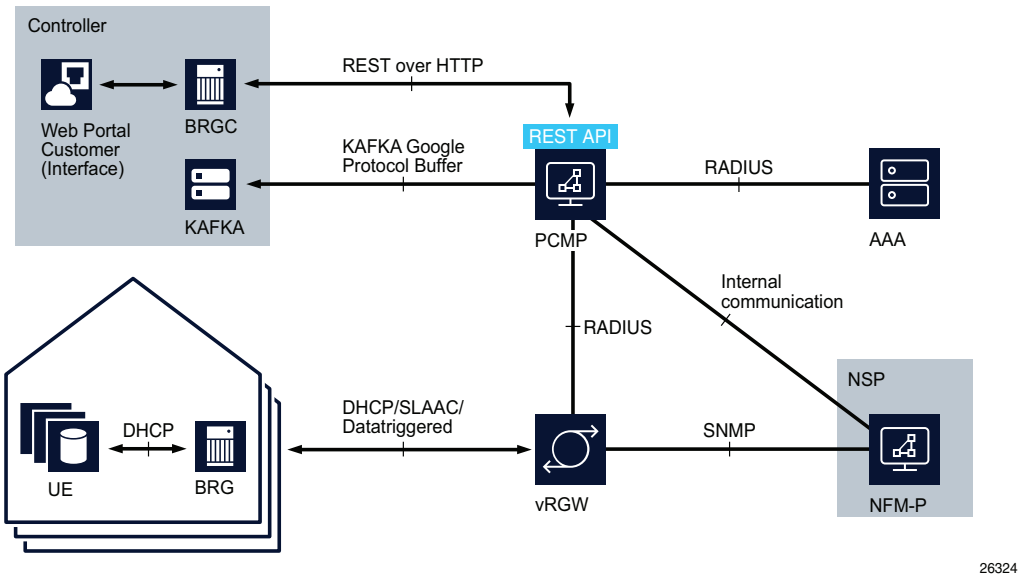
BRGC

A BRGC is a third-party system that maintains a view of the active configuration for each BRG in the network, for example, bandwidth, IP address, and UPnP. The BRGC issues and responds to REST calls to and from the PCMP to apply the configuration to the vRGW.

PCMP architecture

The following diagram displays the PCMP architecture, which is spread among the Nokia PCMP elements and external systems that network operators or third parties maintain using the REST API.

Figure 1-1 PCMP architecture



1.3.10 Internal subcomponents

Internal subcomponents, for example, Java modules, database software, and web server software, are represented by license files in the following directory on a main server:

/opt/nsp/nfmp/server/nms/distribution/licenses

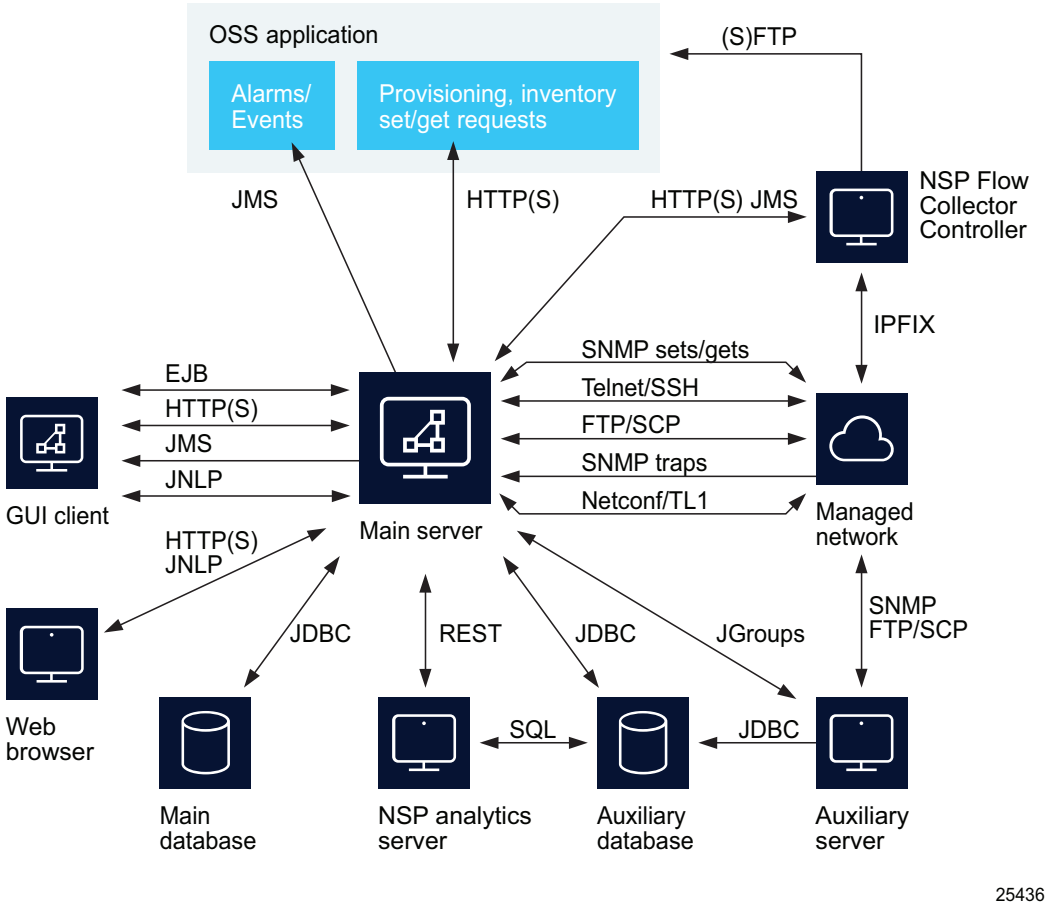
1.4 Component communication

1.4.1 Introduction

The NFM-P component interfaces use industry-standard protocols for communication among servers, databases, NEs, and clients, as shown in Figure 1-2, “NFM-P component communication” (p. 10). NFM-P components communicate with other NFM-P components and external entities using IPv4 or IPv6 exclusively, with the following exceptions:

- The NFM-P can communicate with and manage a network using IPv4 and IPv6 concurrently.
- An NFM-P GUI client or browser-based application client can connect to the NFM-P using IPv4 or IPv6, regardless of the protocol version in use between the NFM-P server and database components.

Figure 1-2 NFM-P component communication



1.4.2 Servers and managed NEs

Main and auxiliary servers send messages to the managed network in the form of SNMP, FTP, secure FTP, and SCP commands. A main server also sends CLI commands using Telnet or SSH.

- A main server uses SNMP to monitor and manage network performance, and to identify network problems. Main servers deploy configuration changes to NEs using SNMP. Auxiliary servers poll MIB performance statistics on the NEs, or collect PCMD or call-trace data. The NEs use asynchronous SNMP messages called traps to notify the NFM-P of events. UDP streaming is used by NEs for operations such as forwarding PCMD records to the NFM-P.
- The CLI of a managed NE is accessible from the client GUI using Telnet or SSH.
- FTP and SCP are transport layer protocols for transferring files between systems. The NFM-P uses the protocols to back up NE configuration data, collect NE accounting statistics, and download software to NEs.

1.4.3 Main server and clients

Client interfaces provide access to an NFM-P system and the managed network through a main server.

A main server and clients communicate in the following ways:

- GUI clients send requests to the server EJB session beans using Java RMI.
- The GUI client update function uses HTTP or HTTPS for client software updates and file downloads.
- NFM-P application clients use HTTP or HTTPS to communicate with the web service on a main server.
- A web-based GUI client communicates through a browser using JNLP.
- XML API OSS clients send requests for processing by a main server, and subscribe to JMS topics to receive real-time event notifications. The messages between a main server and an XML API client are in XML/SOAP format, and are sent over HTTP or HTTPS. The JMS and the XML publisher service on a main server run in separate JVMs to support multiple concurrent client connections. See the *NSP NFM-P XML API Developer Guide* for more information about the messaging between XML API clients and main servers.
- REST API OSS clients perform network management functions and receive notifications using the NFM-P REST API. See the online REST API documentation for information.

1.4.4 Main server and database

A main server communicates with a main database instance using a JDBC session over TCP. JDBC is a Java API for interworking with SQL relational databases.

1.4.5 Main server and auxiliary servers

A main server includes a mechanism for sending requests to auxiliary servers. An auxiliary server notifies the main server after it finishes processing a request. If the main server fails to send a request, or all auxiliary servers are unresponsive to a request, the main server raises an alarm.

1.4.6 NFM-P integration with external systems

The NFM-P can be integrated with external network management systems for purposes such as alarm forwarding. Depending on the external system type, you can use client GUI contextual menu option to open a session on the external system. See the *NSP NFM-P Integration Guide* for information.

1.5 System structure

1.5.1 Introduction

An NFM-P system has a readily adaptable, modular structure that incorporates a relational data model and employs distributed processing.

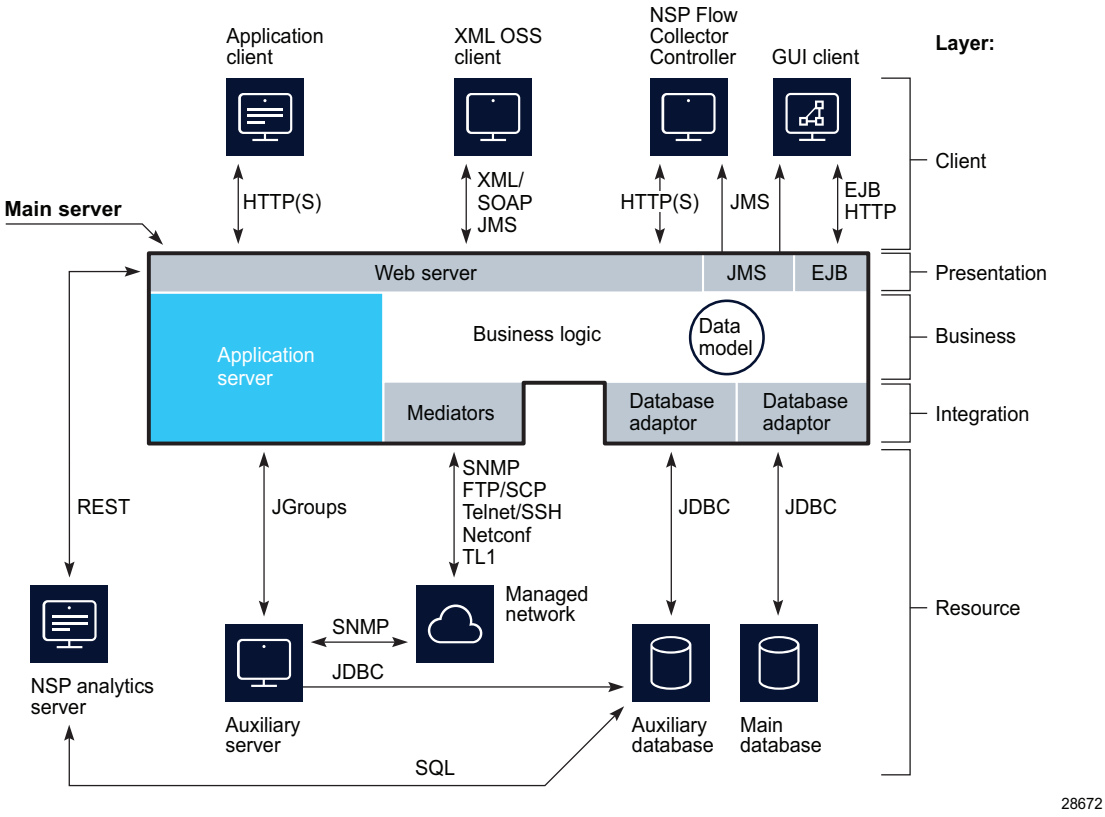
1.5.2 Framework

The NFM-P system elements are created using proprietary and third-party software, and are logically organized in a framework that has the following layers:

- resource
- integration
- business
- presentation
- client

The following figure shows the multi-layer model and the elements in each layer.

Figure 1-3 NFM-P multi-layer model



Resource layer

The resource layer includes the network of managed NEs, the main database, and optional components like auxiliary servers and an auxiliary database. The available resources include, for example, NE configuration backups and software images, ntework topology information, customer service configurations, and statistics.

Integration layer

The integration layer buffers resource-layer elements from the business layer. This layer contains the mediators, which communicate with equipment in the managed network, and the database adapter. The mediator components translate messages from the business layer into the SNMP, FTP, secure FTP, and CLI commands that are sent to the managed network. Messages that are received from the network are processed by the mediator components and passed to the business layer. The database adapter translates business logic requests into JDBC commands, and translates JDBC responses into Java business model objects.

Business layer

The business layer contains the logic and data model for NFM-P functions. The business logic processes client requests, SNMP traps from managed NEs, and internal server events, and performs the appropriate actions on the managed network, clients, and data model, which maintains information about network objects and their relationships. To support the business layer, an application server provides Java EE services.

Presentation layer

The presentation layer buffers the application logic from the client layer. This layer contains several components. The web server receives messages from OSS clients and passes them to the business layer. The application server handles EJB method invocations received from the GUI clients and returns the responses generated by the business-layer logic. The application server also forwards JMS event notification messages from the business layer to GUI and OSS clients.

Client layer

The client layer comprises the GUI, OSS, and web-based application clients. The GUI client Java VM sends EJB RMIs to a main server. The OSS clients send XML/SOAP, or REST messages to a main server. Web clients use JNLP for portal access.

1.5.3 Server data model

The server data model represents the physical and logical elements of the network, such as equipment, customers, services, and statistics. The model also describes the relationships between objects, so allows operators to perform high-level operations that are propagated to child objects, as required. The object associations enable effective central management of large, complex networks.

The NFM-P maintains in the data model a representation of the current managed network state, and incorporates changes as they occur. Changes that are initiated by NEs include event notifications such as fault traps and state changes; changes that are initiated by clients include object creation, deletion, and configuration updates. The changes are applied to the model, saved in the NFM-P database, deployed to the network as required, and reported to clients.

1.5.4 Distributed server architecture

The NFM-P server functions can be distributed across multiple physical or virtual stations in a standalone or redundant configuration.

A main server is the network management engine that monitors the managed network and processes GUI and OSS client requests. A main server also directs the operation of the associated

auxiliary servers and distributes the processing load, as required. The GUI and OSS clients interact only with the currently active main server.

Auxiliary components in a redundant NFM-P system respond to processing requests only from the current primary main server. Depending on the system configuration, if the main servers change roles because of a failure or deliberate operator action, an auxiliary server begins to take requests from the new primary main server, or remains idle as the main server directs the requests to other auxiliary servers.

A main server sends new or updated operating information such as the NFM-P license capacity, redundancy status, or database credentials, to each required auxiliary component as the information becomes available.

1.6 Security

1.6.1 Platform security

The RHEL OS that is common to all NFM-P components is protected from attack using firewalls and stringent internal security measures that restrict access to files and functions. Appendix A, “NFM-P DISA STIG compliance” describes the NFM-P RHEL OS compliance with the Security Technical Implementation Guide (STIG) benchmarks of the U.S. Defense Information Systems Agency (DISA).

1.6.2 Communication security

The NFM-P employs strict security at the session and other communication layers. Interfaces between a main server and other system components are secured using Transport Layer Security, or TLS.

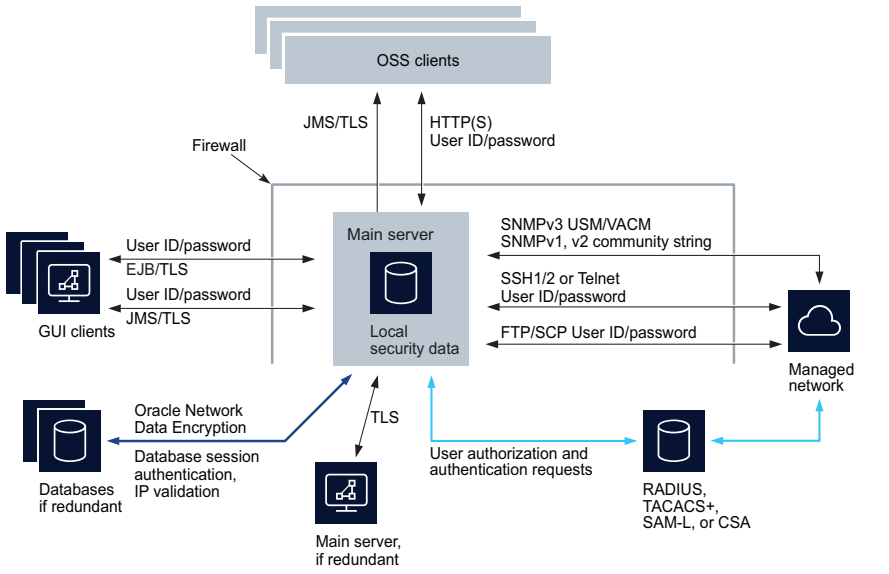
Communication with a main database is secured using Oracle Network Data Encryption.

A GUI, application, or OSS client must provide user credentials for access to the NFM-P. Session credentials and messages are protected using mechanisms and protocols that include the following:

- HTTPS, as the application-layer transport for clients
- SSH, SCP, and SNMPv3 with USM or VACM, at the application layer for communication between a main server and the managed network
- NAT, at the network layer, between the following:
  - main server and single-user GUI client or client delegate server
  - main or auxiliary server and OSS client
  - main or auxiliary server and managed network
- IP validation, at the network layer, between the main or other server components and each main database

The following figure shows the NFM-P components and the security mechanisms.

Figure 1-4 NFM-P security mechanisms



1.6.3 Session management

Effective session management requires authentication, authorization, and accounting, or AAA. Authentication is the verification of user credentials. Authorization is the assignment of access privileges to users. Accounting is the recording of user actions. An NFM-P operator can configure AAA functions using the local NFM-P security mechanisms, a third-party server, or both.

- Local NFM-P authentication is performed using a local database of users and a local security scheme.
- Supported third-party authentication servers are RADIUS, TACACS+, LDAP, SAM-L, and CSA, which run on separate platforms, and have separate user lists and administration processes.

NFM-P user accounts consist of a user name, password, and an associated user group, scope of command, and span of control. User groups define user authorization levels, and control the level of access to objects such as equipment, customers, services, and alarms. An NFM-P administrator can limit the type of user access per managed NE; for example, allowing FTP access but denying console, Telnet, or SNMP access.

Client sessions

All client sessions require authentication.

- A GUI client EJB session is authenticated using the client username and password.
- An OSS client session is authenticated using cached information from an authorization server.
- A JMS session is authenticated using the client username and password.

Database sessions

A main database is accessible through a connection that is secured by a user name and password. After each database update in response to a GUI or OSS client request, the client activity log records the request information, which includes the name of the associated NFM-P user.

Secure communication between a main server and database is available using the IP validation function, which is typically configured on a main database station during an installation or upgrade.

Managed NE sessions

A main or auxiliary server opens CLI, FTP, SFTP and SCP sessions on managed NEs. A managed NE uses a local security database, or a third-party service such as RADIUS or TACACS+, to perform AAA functions.

SNMPv3 message authentication and authorization are handled by the USM and VACM mechanisms, which define the user authorization permissions. Older SNMP versions are authenticated using community strings. Each SNMP message is individually authenticated.

1.6.4 Network transport security

Transport-layer security is available to the network protocols that carry messages between NFM-P components.

Main server and clients

Communication between a main server and clients is performed using messaging such as the following.

- XML API clients use HTTP or HTTPS to send XML/SOAP messages, and receive notifications using JMS, which can be secured using TLS.
- REST API clients use HTTPS.
- GUI clients use the EJB interface, which can be secured using TLS.

Servers and managed NEs

A managed NE communicates with a main or auxiliary server using SNMP, FTP, SCP, or UDP. When SNMPv3 is used, an SHA or MD5 authentication key is included in each message and checked against the shared encryption key.

SSH provides the security for a CLI session between a GUI client and a managed NE.

RSA encryption is available for communication between auxiliary servers and managed NEs. Contact customer support for information.

Firewall support

The NFM-P supports firewall deployment on all server interfaces; for example, between a main server and the auxiliary servers, GUI, and OSS clients, and between a main or auxiliary server and the managed network. See the *NSP NFM-P Planning Guide* for firewall and reserved TCP port information.

1.7 Fault tolerance

1.7.1 Introduction

Fault tolerance provides system reliability by maintaining availability in the event of a component failure. NFM-P fault tolerance includes high availability using component redundancy. Deploying redundant NFM-P hardware and software components ensures that there is no single point of NFM-P system failure.

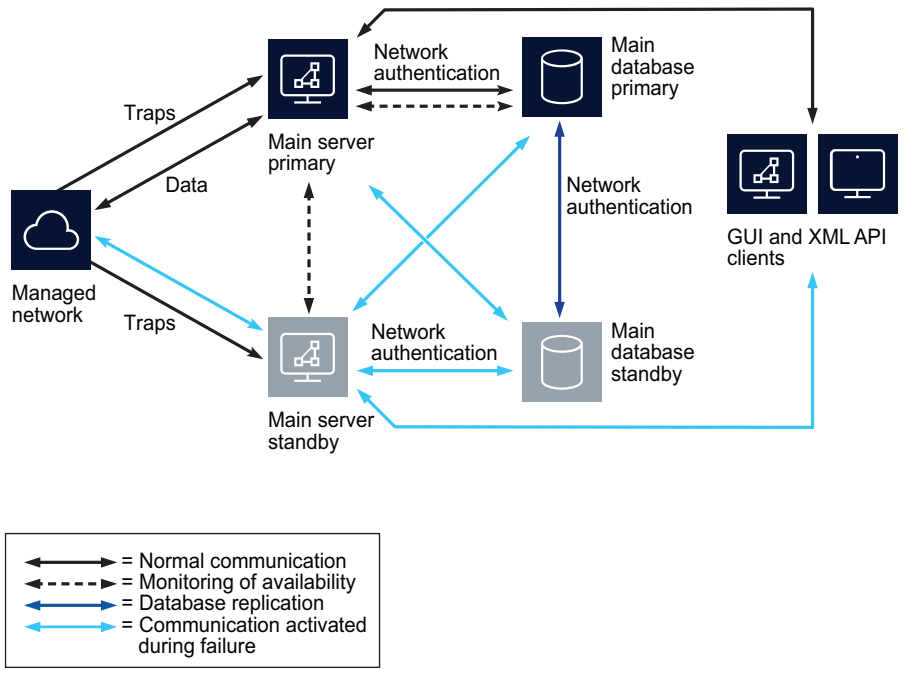
Redundant physical network interfaces and points of network entry ensure that there is no single point of failure between the NFM-P system and the managed network. Redundant network paths, for example, in-band and out-of-band management, can help to prevent the isolation of a main server from the network in the event of a routing failure.

See the “NFM-P system redundancy” chapter of the *NSP NFM-P Administrator Guide* for more information.

1.7.2 Main server and database redundancy

A redundant NFM-P system consists of a primary main server and primary main database that actively manage the network, and a second main server and database in warm standby mode. A main server and database can be collocated on one station, or distributed on separate stations. The following figure shows a distributed NFM-P system deployed in a redundant configuration.

Figure 1-5 Redundant NFM-P system



Main server redundancy

Main server redundancy is achieved using clustering technology provided by a JBOSS application server on each main server. The primary and standby main servers regularly poll each other to monitor availability. Traps from the managed network are always sent to both main servers in order to avoid delays in the event that a main server fails.

If the primary server loses visibility of the standby server, it notifies the GUI clients. If the standby server loses visibility of the primary server, the standby server attempts to become the primary server by connecting to the primary database.

NFM-P database redundancy

NFM-P database redundancy uses Oracle Data Guard Replication in real-time apply mode to keep the standby database synchronized with data changes in the primary database. The supported fault-recovery operations are database switchovers and database failovers. A switchover is a manual operation that switches the primary and standby database roles. A failover is an automatic operation that forces the standby database to become the primary database when a primary main database failure is detected.

The primary main server regularly polls each main database. If the primary or standby database is unavailable, the main server notifies the GUI clients. If both main servers lose contact with the primary main database, a failover occurs and the standby main database becomes the primary.

1.7.3 Auxiliary servers and NFM-P redundancy

Auxiliary servers are passively redundant. They do not cause or initiate main server or database redundancy activities, but if a Preferred auxiliary server ceases to respond to requests from the primary main server and a Reserved auxiliary server is available, the main server directs the current and subsequent requests to the Reserved auxiliary server until the Preferred auxiliary server is available.

An auxiliary server communicates only with the current primary server and database. After an NFM-P redundancy activity such as a database failover, the primary main server directs the auxiliary servers to communicate with the current primary component instead of the former primary component.

1.8 Standards compliance

1.8.1 Description

The NFM-P system uses industry standards and open-standard interfaces that allow the system to interoperate with a variety of other network monitoring and management systems. The following table lists the NFM-P compliance with various standards:

Table 1-1 NFM-P standards compliance

Standard	Description
3GPP	3rd Generation Partnership Project IRPs for CORBA R8 and SOAP/XML R8 Solution Sets

Table 1-1 NFM-P standards compliance (continued)

Standard	Description
draft-grant-tacacs-02.txt	TACACS+ client
draft-ylonen-ssh-protocol-00.txt	SSH
EJB	Java EE Enterprise Java Session Bean version 2.1
HTML5	HyperText Markup Language 5, for NFM-P applications
HTTP(S)	HyperText Transfer Protocol (Secure) version 1.1
ITU-T X.721	SMI
ITU-T X.734	Event report management function
Java SE	Java Standard Edition version 8
JBOSS EAP	Java Bean Open Source Software Enterprise Application Platform version 7
JMS	Java Message Service version 1.1
JSON	ECMA-404 JavaScript Object Notation Data Interchange Format
JS/ECMAScript 5	ECMA-262 ECMA Script Language Specification
M.3100/3120	Equipment and connection models
MTOSI	Compliance of generic network objects, inventory retrieval, and JMS over XML
RFC 0959	FTP
RFC 1213	SNMPv1
RFC 1738	Uniform Resource Locators (URL)
RFC 2138	RADIUS client 2618
RFC 3411-3415	SNMPv3
RFC 3416	SNMPv2c
RFC 5246	The Transport Layer Security (TLS) Protocol
RFC 6241	Network Configuration Protocol (NETCONF)
SAML	SAM-L 1.1
SOAP	W3C SOAP 1.2
TMF 509/613	Network connectivity model
TR-069	TR-069 (Amendment 1) by way of the Home Device Manager
XML	W3C XML 1.0
	W3C Namespaces in XML
	W3C XML schemas

The following standards are considered in the NFM-P GUI design:

- Sun Microsystems, *Java Look and Feel Design Guidelines*, Addison-Wesley Publishing Company, Reading, Massachusetts 1999
- ANSI T1.232-1996, *Operations, Administration, and Provisioning (OAM&P)- G Interface Specifications for Use with the Telecommunications Management Network (TMN)*
- Telcordia (Bell Core) GR-2914-CORE Sept. 98, *Human Factors Requirements for Equipment to Improve Network Integrity*
- Telcordia (Bell Core) GR-826-CORE, June 1994, Issue 1, Section 10.2 of OTGR, *User Interface Generic Requirements for Supporting Network Element Operations*
- ITU-T Recommendation Z.361 (02/99), *Design guidelines for Human- Computer Interfaces (HCI) for the management of telecommunications networks*
- ETSI EG 201 204 v1.1.1 (1997-05), *Human Factors (HF); User Interface design principles for the Telecommunications Management Network (TMN) applicable to the “G” Interface*
- 3GPP 32-series R8 specification, published December, 2009.

A NFM-P DISA STIG compliance

A.1 NFM-P RHEL OS compliance with DISA STIG benchmarks

A.1.1 NFM-P RHEL 7 OS compliance

Table A-1, "DISA STIG benchmarks and NFM-P RHEL 7 OS compliance" (p. 21) lists the Security Technical Implementation Guide (STIG) benchmarks of the U.S. Defense Information Systems Agency (DISA), and the NFM-P RHEL 7 OS compliance with each.

The following compliance indicators are used:

- Supported—The product is fully compliant with the recommendation.
- No expected impact—The product team has not explicitly tested using the recommended configuration, but foresees no effect on system functions.

  It is recommended that you test such a configuration to ensure that system operation is unaffected; no commitment is offered to ensure product compatibility with a specific requirement.
- Partially supported—The product is conditionally compliant with the recommendation, as described in the Notes column.
- Not supported—The product does not support the recommended configuration.

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-010010	Verify package integrity	High	Not supported	—
RHEL-07-010020	Verify file hashes with RPM	High	Not supported	The NFM-P modifies files during regular installation and operation.
RHEL-07-010030	Ensure GDM login banner is configured	Medium	Supported	—
RHEL-07-010040	Set GNOME3 login warning banner text	Medium	Supported	—
RHEL-07-010050	Ensure local login warning banner is configured properly	Medium	Supported	—
RHEL-07-010060	Enable GNOME3 screen saver lock after idle period	Medium	Supported	—
RHEL-07-010061	Enable GNOME3 login smart-card authentication	Medium	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-010062	Ensure users cannot change GNOME3 screen saver lock after idle period	Medium	Supported	—
RHEL-07-010070	Set GNOME3 screen saver inactivity timeout	Medium	Supported	—
RHEL-07-010081	Ensure users cannot change GNOME3 screen saver settings	Medium	Supported	—
RHEL-07-010082	Ensure users cannot change GNOME3 session idle settings	Medium	Supported	—
RHEL-07-010090	Install screen package	Medium	Supported	—
RHEL-07-010100	Enable GNOME3 screen saver idle activation	Medium	Supported	—
RHEL-07-010101	Ensure users cannot change GNOME3 screen saver idle activation	Medium	Supported	—
RHEL-07-010110	Set GNOME3 screen saver lock delay after activation period	Medium	Supported	—
RHEL-07-010119	Set password retry prompts permitted per session	Unknown	Supported	—
RHEL-07-010120	Set password strength minimum uppercase characters	Medium	Supported	—
RHEL-07-010130	Set password strength minimum lowercase characters	Medium	Supported	—
RHEL-07-010140	Set password strength minimum digit characters	Medium	Supported	—
RHEL-07-010150	Set password strength minimum special characters	Medium	Supported	—
RHEL-07-010160	Set password strength minimum different characters	Medium	Supported	—
RHEL-07-010170	Set password strength minimum different categories	Medium	Supported	—
RHEL-07-010180	Set password maximum consecutive repeating characters	Medium	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-010190	Set password to maximum of consecutive repeating characters from same character class	Medium	Supported	—
RHEL-07-010200	Set PAM password hashing algorithm	Medium	Supported	—
RHEL-07-010210	Set password hashing algorithm in /etc/login.defs	Medium	Supported	—
RHEL-07-010220	Set password hashing algorithm in /etc/libuser.conf	Medium	Supported	—
RHEL-07-010230	Set password minimum age	Medium	Supported	—
RHEL-07-010240	Set existing passwords minimum age	Medium	Supported	—
RHEL-07-010250	Ensure password expiration is 90 days or less	Medium	Partially supported	NOTE: Must not be altered for NSP UNIX users.
RHEL-07-010260	Set existing passwords maximum age	Medium	Supported	—
RHEL-07-010270	Ensure password reuse is limited	Medium	Supported	—
RHEL-07-010280	Set password minimum length	Medium	Supported	—
RHEL-07-010290	Prevent login to accounts with empty password	High	Supported	—
RHEL-07-010300	Ensure SSH PermitEmptyPass-words is disabled	High	Supported	—
RHEL-07-010310	Set account expiration following inactivity	Medium	Supported	—
RHEL-07-010320	Ensure lockout for failed password attempts is configured	Medium	Supported	—
RHEL-07-010330	Configure root account for failed password attempts	Medium	Supported	—
RHEL-07-010340	Ensure users re-authenticate for privilege escalation - sudo NOPASSWD	Medium	Supported	—
RHEL-07-010350	Ensure users re-authenticate for privilege escalation - sudo !authenticate	Medium	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-010430	Ensure logon failure delay is set correctly in login.defs	Unknown	Supported	—
RHEL-07-010440	Disable GDM automatic login	High	Supported	—
RHEL-07-010450	Disable GDM guest login	High	Supported	—
RHEL-07-010460	Ensure SSH PermitUserEnvironment is disabled	Medium	Supported	—
RHEL-07-010470	Ensure SSH HostbasedAuthentication is disabled	Medium	Supported	—
RHEL-07-010480	Set boot loader password in grub2	High	Supported	—
RHEL-07-010481	Ensure authentication required for single-user mode	Medium	Supported	—
RHEL-07-010490	Ensure bootloader password is set	Medium	Supported	—
RHEL-07-010500	Enable smart-card login	Medium	Supported	—
RHEL-07-020000	Uninstall rsh-server package	High	Supported	—
RHEL-07-020010	Ensure NIS server is not enabled	High	Supported	—
RHEL-07-020020	Map system users to appropriate SELinux role	Medium	Not supported	—
RHEL-07-020030	Ensure file system integrity regularly checked	Medium	Not supported	Requires AIDE
RHEL-07-020040	Configure notification of post-AIDE scan details	Medium	Not supported	—
RHEL-07-020050	Ensure gpgcheck is globally activated	High	Not supported	NSP packages are unsigned and will fail to install.
RHEL-07-020060	Ensure gpgcheck enabled for local packages	High	Not supported	NSP packages are unsigned and will fail to install.
RHEL-07-020070	Ensure gpgcheck enabled for repository metadata	High	Supported	—
RHEL-07-020100	Disable modprobe loading of USB storage driver	Medium	Supported	—
RHEL-07-020101	Ensure DCCP is disabled	Medium	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-020110	Disable automounting	Medium	Supported	—
RHEL-07-020200	Ensure yum removes previous package versions	Low	Supported	—
RHEL-07-020210	Ensure SELinux state is enforcing	High	Not supported	SELinux is not supported.
RHEL-07-020220	Ensure SELinux policy is configured	High	Not supported	SELinux is not supported.
RHEL-07-020230	Disable Ctrl-Alt-Del reboot activation	High	Supported	—
RHEL-07-020240	Ensure default umask set correctly in login.defs	Unknown	Supported	—
RHEL-07-020250	Ensure installed operating system vendor-supported and certified	High	Supported	Maintenance is provided only for RHEL qcow2 images.
RHEL-07-020260	Ensure updates, patches, and additional security software are installed	High	Partially supported	Applying RHEL patches is supported, but any compatibility issues require backing out RHEL updates until a fix is available. Nokia does not recommend installing any additional software on the OS that hosts the NSP, as it may impact NSP operation. Any non-sanctioned software must be removed if suspected of causing NSP issues.
RHEL-07-020300	All GIDs referenced in /etc/passwd are defined in /etc/group	Low	Supported	—
RHEL-07-020310	Verify only root has UID 0	High	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-020320	Ensure no unowned files or directories exist	Medium	Supported	—
RHEL-07-020330	Ensure no ungrouped files or directories exist	Medium	Supported	—
RHEL-07-020600	All interactive users have home directory defined	Medium	Supported	—
RHEL-07-020610	Ensure home directories created for new users	Medium	Supported	—
RHEL-07-020620	All interactive user home directories exist	Medium	Supported	—
RHEL-07-020630	All Interactive user home directories have mode 0750 or less permissive	Medium	Not supported	—
RHEL-07-020640	All Interactive user home directories owned by primary user	Medium	Not supported	—
RHEL-07-020650	All Interactive user home directories group-owned by primary user	Medium	Not supported	—
RHEL-07-020660	All user files and directories In home directory owned by primary user	Medium	Not supported	—
RHEL-07-020670	All user files and directories in home directory group-owned by primary user	Medium	Not supported	—
RHEL-07-020680	All user files and directories In home directory have mode 0750 or less permissive	Medium	Not supported	—
RHEL-07-020690	User initialization files owned by primary user	Medium	Not supported	—
RHEL-07-020700	User initialization files group-owned by primary user	Medium	Not supported	—
RHEL-07-020710	All user initialization files have mode 0740 or less permissive	Medium	Not supported	—
RHEL-07-020720	Ensure that user path contains only local directories	Medium	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-020730	User initialization files must not run world-writable programs	Medium	Supported	—
RHEL-07-020900	Ensure no device files are unlabeled by SELinux	Medium	Not supported	—
RHEL-07-021000	Ensure nodev option set on /tmp partition	Unknown	Supported	—
RHEL-07-021010	Ensure nosuid option set on removable media partitions	Unknown	Supported	Supported, but may impact ability to install NSP or patches from DVD drive or USB device
RHEL-07-021020	Mount remote filesystems with nosuid	Medium	Supported	—
RHEL-07-021021	Mount remote filesystems with noexec	Medium	Supported	—
RHEL-07-021030	Ensure all world-writable directories are owned by a system account	Unknown	Not supported	—
RHEL-07-021040	Ensure default umask set correctly for interactive users	Medium	Not supported	NFM-P sets umask for interactive users
RHEL-07-021100	Ensure cron logs to rsyslog	Medium	Supported	—
RHEL-07-021110	Verify user who owns /etc/cron.allow file	Medium	Supported	—
RHEL-07-021120	Verify group who owns /etc/cron.allow file	Medium	Supported	—
RHEL-07-021300	Disable KDump kernel crash analyzer (kdump)	Medium	Supported	—
RHEL-07-021310	Ensure separate partition exists for /home	Low	Supported	Customer to determine appropriate size; disk space cannot be taken from other partitions defined in installation guide

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-021320	Ensure separate partition exists for /var	Low	Supported	Customer to determine appropriate size; disk space cannot be taken from other partitions defined in installation guide
RHEL-07-021330	Ensure separate partition exists for /var/log/audit	Low	Supported	Customer to determine appropriate size; disk space cannot be taken from other partitions defined in installation guide
RHEL-07-021340	Ensure separate partition exists for /tmp	Low	Supported	Customer to determine appropriate size; disk space cannot be taken from other partitions defined in installation guide
RHEL-07-021350	Enable FIPS mode in GRUB2	High	Supported	Ensure openSSL is enabled and running
RHEL-07-021600	Configure AIDE to verify ACLs	Medium	Not supported	—
RHEL-07-021610	Configure AIDE to verify extended attributes	Medium	Not supported	—
RHEL-07-021620	Configure AIDE to use FIPS 140-2 for validating hashes	Medium	Not supported	—
RHEL-07-021700	Boat loader not Installed on removable media	Medium	Supported	—
RHEL-07-021710	Ensure chargen services are disabled	High	Supported	—
RHEL-07-030000	Ensure auditd service is enabled	High	Supported	—
RHEL-07-030010	Shut down system when auditing failures occur	Medium	Supported	Supported but not recommended
RHEL-07-030300	Configure audispd plugin to send logs to remote server	Medium	Not supported	May impact system performance

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-030310	Encrypt audit records sent with audispd plugin	Medium	Not supported	May impact system performance
RHEL-07-030320	Configure audispd's plugin disk_full_action when disk full	Medium	Not supported	May impact system performance
RHEL-07-030321	Configure audispd's plugin network_failure_action on network failure	Medium	Not supported	May impact system performance
RHEL-07-030330	Configure auditd space_left on low disk space	Medium	Supported	—
RHEL-07-030350	Configure auditd mail_acct action on low disk space	Medium	Supported	May impact system performance
RHEL-07-030360	Ensure auditd collects information on use of privileged commands	Medium	Supported	See equiv CIS - 4.1.12
RHEL-07-030370	Record events that modify system discretionary access controls - chown	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030380	Record events that modify system discretionary access controls - fchown	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030390	Record events that modify system discretionary access controls - lchown	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030400	Record events that modify system discretionary access controls - fchownat	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030410	Record events that modify system discretionary access controls - chmod	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030420	Record events that modify system discretionary access controls - fchmod	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030430	Record events that modify system discretionary access controls - fchmodat	Unknown	Supported	See equiv CIS - 4.1.10

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-030440	Record events that modify system discretionary access controls - setxattr	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030450	Record events that modify system discretionary access controls - fsetxattr	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030460	Record events that modify system discretionary access controls - lsetxattr	Unknown	Supported	See equiv CIS - 4.1.10
RHEL-07-030470	Record events that modify system discretionary access controls - removexattr	Medium	Supported	See equiv CIS - 4.1.10
RHEL-07-030480	Record events that modify system discretionary access controls - fremovexattr	Medium	Supported	See equiv CIS - 4.1.10
RHEL-07-030490	Record events that modify system discretionary access controls - lremovexattr	Medium	Supported	See equiv CIS - 4.1.10
RHEL-07-030500	Record unauthorized access attempts to files (unsuccessful) - create	Medium	Supported	See equiv CIS - 4.1.11
RHEL-07-030510	Record unauthorized access attempts to files (unsuccessful) - open	Medium	Supported	See equiv CIS - 4.1.11
RHEL-07-030520	Record unauthorized access attempts to files (unsuccessful) - openat	Medium	Supported	See equiv CIS - 4.1.11
RHEL-07-030530	Record unauthorized access attempts to files (unsuccessful) - open_by_handle_at	Medium	Supported	See equiv CIS - 4.1.11
RHEL-07-030540	Record unauthorized access attempts to files (unsuccessful) - truncate	Medium	Supported	See equiv CIS - 4.1.11
RHEL-07-030550	Record unauthorized access attempts to files (unsuccessful) - ftruncate	Medium	Supported	See equiv CIS - 4.1.11

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-030560	Record any attempt to run semanage	Medium	Supported	SELinux is not supported.
RHEL-07-030570	Record any attempt to run setsebool	Medium	Supported	SELinux is not supported.
RHEL-07-030580	Record any attempt to run chcon	Medium	Supported	—
RHEL-07-030590	Record any attempt to run setfiles	Medium	Supported	—
RHEL-07-030600	Record attempts to alter logon and logout events - tallylog	Medium	Supported	—
RHEL-07-030610	Record attempts to alter logon and logout events - faillock	Medium	Supported	See equiv CIS - 4.1.8
RHEL-07-030620	Record attempts to alter logon and logout events - lastlog	Medium	Supported	See equiv CIS - 4.1.8
RHEL-07-030630	Ensure auditd collects information on use of privileged commands - passwd	Medium	Supported	—
RHEL-07-030640	Ensure auditd collects information on use of privileged commands - unix_chkpwd	Medium	Supported	—
RHEL-07-030650	Ensure auditd collects information on use of privileged commands - gpasswd	Medium	Supported	—
RHEL-07-030660	Ensure auditd collects information on use of privileged commands - chage	Medium	Supported	—
RHEL-07-030670	Ensure auditd collects information on use of privileged commands - userhelper	Medium	Supported	—
RHEL-07-030680	Ensure auditd collects information on use of privileged commands - su	Medium	Supported	—
RHEL-07-030690	Ensure auditd collects information on use of privileged commands - sudo	Medium	Supported	—
RHEL-07-030700	Ensure auditd Collects System Administrator Actions	Unknown	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-030710	Ensure auditd collects information on use of privileged commands - newgrp	Medium	Supported	—
RHEL-07-030720	Ensure auditd collects information on use of privileged commands - chsh	Medium	Supported	—
RHEL-07-030730	Ensure auditd collects information on use of privileged commands - sudoedit	Medium	Supported	—
RHEL-07-030740	Ensure SSH idle timeout interval is configured	Medium	Not supported	OSS clients could be impacted.
RHEL-07-030750	Ensure auditd collects information on use of privileged commands - umount	Medium	Supported	—
RHEL-07-030760	Ensure auditd collects information on use of privileged commands - postdrop	Medium	Supported	—
RHEL-07-030770	Ensure auditd collects information on use of privileged commands - postqueue	Medium	Supported	—
RHEL-07-030780	Ensure auditd collects information on use of privileged commands - ssh-keysign	Medium	Supported	—
RHEL-07-030800	Ensure auditd collects information on use of privileged commands - crontab	Medium	Supported	—
RHEL-07-030810	Ensure auditd collects information on use of privileged commands - pam_timestamp_ check	Medium	Supported	—
RHEL-07-030819	Ensure auditd collects information on kernel module loading - create_module	Medium	Supported	—
RHEL-07-030820	Ensure auditd collects information on kernel module loading - init_module	Medium	Supported	See equiv CIS - 4.1.17

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-030821	Ensure auditd collects information on kernel module loading and unloading - finit_module	Medium	Supported	May impact system performance
RHEL-07-030830	Ensure auditd collects information on kernel module unloading - delete_module	Medium	Supported	See equiv CIS - 4.1.17
RHEL-07-030840	Ensure auditd collects information on kernel module loading - insmod	Medium	Supported	See equiv CIS - 4.1.17
RHEL-07-030850	Ensure auditd collects information on kernel module unloading - rmmod	Medium	Supported	May impact system performance; see equiv CIS - 4.1.17
RHEL-07-030860	Ensure auditd collects information on kernel module loading and unloading - modprobe	Medium	Supported	See equiv CIS - 4.1.17
RHEL-07-030870	Record events that modify user/group information - /etc/passwd	Medium	Supported	See equiv CIS - 4.1.5
RHEL-07-030871	Record events that modify user/group information - /etc/group	Medium	Supported	See equiv CIS - 4.1.5
RHEL-07-030872	Record events that modify user/group information - /etc/gshadow	Medium	Supported	See equiv CIS - 4.1.5
RHEL-07-030873	Record events that modify user/group information - /etc/shadow	Medium	Supported	See equiv CIS - 4.1.5
RHEL-07-030874	Record events that modify user/group information - /etc/security/opasswd	Medium	Supported	See equiv CIS - 4.1.5
RHEL-07-030880	Ensure auditd collects file deletion events by user - rename	Medium	Supported	See equiv CIS - 4.1.14
RHEL-07-030890	Ensure auditd collects file deletion events by user - renameat	Medium	Supported	See equiv CIS - 4.1.14

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-030900	Ensure auditd collects file deletion events by user - rmdir	Medium	Supported	—
RHEL-07-030910	Ensure auditd collects file deletion events by user - unlink	Medium	Supported	See equiv CIS - 4.1.14
RHEL-07-030920	Ensure auditd collects file deletion events by user - unlinkat	Medium	Supported	See equiv CIS - 4.1.14
RHEL-07-031000	Ensure logs sent to remote host	Unknown	Supported	—
RHEL-07-031010	Ensure rsyslog does not accept remote messages unless acting as log server	Unknown	Supported	—
RHEL-07-032000	Install McAfee virus scanning software	High	Not supported	—
RHEL-07-032010	Virus scanning software definitions are updated	Medium	Not supported	—
RHEL-07-040000	Limit number of concurrent login sessions allowed per user	Low	Not supported	—
RHEL-07-040100	Configure firewalld ports	Medium	Supported	—
RHEL-07-040110	Use only FIPS 140-2 validated ciphers	Medium	Supported	Ensure openSSL is enabled and running.
RHEL-07-040160	Set interactive session timeout	Medium	Not supported	OSS clients could be impacted.
RHEL-07-040170	Ensure SSH warning banner is configured	Medium	Supported	—
RHEL-07-040180	Configure SSSD LDAP backend to use TLS for all transactions	Medium	No expected impact	—
RHEL-07-040190	Configure SSSD LDAP backend client CA certificate location	Medium	No expected impact	—
RHEL-07-040200	Configure SSSD LDAP backend client CA certificate	Medium	No expected impact	—
RHEL-07-040201	Ensure core dumps are restricted	Medium	Not supported	Core files are required in order to provide software support for customers.
RHEL-07-040300	Install OpenSSH server package	Medium	Supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-040310	Enable OpenSSH service	Medium	Supported	—
RHEL-07-040320	Set SSH idle timeout Interval	Unknown	Supported	—
RHEL-07-040330	Disable SSH support for rhosts RSA authentication	Medium	Not supported	Not compatible with NSP installer
RHEL-07-040340	Ensure only approved MAC algorithms are used	Medium	Supported	NOTE: If eNodeB NEs are managed, hmac-sha1 must be included as well.
RHEL-07-040350	Ensure SSH IgnoreRhosts is enabled	Medium	Supported	—
RHEL-07-040360	Print last log	Medium	Supported	—
RHEL-07-040370	Ensure SSH root login is disabled	Medium	Supported	—
RHEL-07-040380	Disable SSH support for user known hosts	Medium	Not supported	Not compatible with NSP installer
RHEL-07-040390	Ensure SSH protocol is set to 2	High	Supported	—
RHEL-07-040400	Use only FIPS 140-2 validated MACs	Medium	Supported	Ensure openSSL is enabled and running
RHEL-07-040410	Verify permissions on SSH server public *.pub key files	Medium	Supported	—
RHEL-07-040420	Verify permissions on SSH server private *_key key files	Medium	Supported	—
RHEL-07-040430	Disable GSSAPI authentication	Medium	Supported	—
RHEL-07-040440	Disable Kerberos authentication	Medium	Supported	—
RHEL-07-040450	Enable use of strict mode checking	Medium	Supported	—
RHEL-07-040460	Enable use of privilege separation	Medium	Supported	—
RHEL-07-040470	Disable compression or set compression to delayed	Medium	Supported	May not be possible for all networks
RHEL-07-040500	Configure time service maxpoll interval	Unknown	Supported	—
RHEL-07-040510	Configure firewalld to rate-limit connections	Medium	Not supported	—

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-040520	Verify firewalld enabled	Medium	—	—
RHEL-07-040530	Set last logon/access notification	Low	Supported	—
RHEL-07-040540	Remove user host-based authentication files	High	Not supported	Not compatible with NSP installer
RHEL-07-040550	Remove host-based authentication files	High	Not supported	Not compatible with NSP installer
RHEL-07-040600	Configure multiple DNS servers in /etc/resolv.conf	Unknown	Supported	—
RHEL-07-040610	Configure kernel parameter for accepting IPv4 source-routed packets for all interfaces	Medium	Supported	See equiv CIS - 3.2.1
RHEL-07-040620	Ensure source-routed packets are not accepted	Medium	Supported	—
RHEL-07-040630	Ensure broadcast ICMP requests are ignored	Medium	Supported	—
RHEL-07-040640	Configure kernel parameter for accepting ICMP redirects by default	Medium	Supported	See equiv CIS - 3.2.2
RHEL-07-040641	Ensure ICMP redirects are not accepted	Medium	Supported	—
RHEL-07-040650	Disable kernel parameter for sending ICMP redirects by default	Medium	Supported	See equiv CIS - 3.1.2
RHEL-07-040660	Ensure packet redirect sending is disabled	Medium	Supported	—
RHEL-07-040670	Ensure system is not acting as a network sniffer	Medium	Supported	—
RHEL-07-040680	Prevent unrestricted mail relaying	Medium	Supported	—
RHEL-07-040690	Uninstall vsftpd package	High	Supported	—
RHEL-07-040700	Uninstall tftp-server Package	High	Supported	—
RHEL-07-040710	Ensure SSH X.11 forwarding is disabled	High	Supported	Supported; SSH X.11 forwarding impacts GUI clients

Table A-1 DISA STIG benchmarks and NFM-P RHEL 7 OS compliance (continued)

DISA STIG benchmark	Recommendation	Severity	Compliance	Notes
RHEL-07-040720	Ensure tftp daemon uses secure mode	Medium	Supported	tftp not recommended
RHEL-07-040730	Ensure X Window system is not installed	Medium	Supported	May impact ability to run GUI client locally on NSP server
RHEL-07-040740	Ensure IP forwarding is disabled	Medium	Supported	—
RHEL-07-040750	Mount remote filesystems with Kerberos security	Medium	No expected impact	—
RHEL-07-040800	Ensure default SNMP password is not used	High	Supported	—
RHEL-07-040810	Set default firewalld aone for incoming packets	Medium	Supported	—
RHEL-07-040820	Verify any configured IPSec tunnel connections	Medium	No expected impact	—
RHEL-07-040830	Configure Kernel parameter for accepting IPv6 source-routed packets for all interfaces	Medium	Supported	—
RHEL-07-041001	Install smart-card packages for multi-factor authentication	Medium	Supported	—
RHEL-07-041002	Configure PAM in SSSD services	Medium	No expected impact	—
RHEL-07-041003	Configure smart-card certificate status checking	Medium	Supported	—
RHEL-07-041010	Deactivate wireless network interfaces	Medium	Supported	—
RHEL-07-TBD	Verify and correct ownership with RPM	High	Supported	—